The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
2011-09-13

SUBJECT:
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS11-073)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Office which is Microsoft's business application suite. These vulnerabilities can be exploited by opening a specially crafted Office file or a legitimate Office file that is located in the same network directory as a specially crafted library file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user.

Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Two vulnerabilities have been identified in Microsoft Office that could allow remote code execution.

A vulnerability exists in Microsoft Word due to an uninitialized object pointer in the MSO.dll file. This vulnerability can be triggered by opening a specially crafted Word file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted Word file as an email attachment. In the web based scenario, a user would have to open the specially crafted Word file that is hosted on a website. When the user opens the Word file, the attacker's supplied code will execute.

An additional vulnerability exists due to incorrect path restrictions while loading Microsoft Office Word, Excel, or PowerPoint dynamic link library (DLL) files. To exploit this vulnerability, an attacker could create a specially crafted DLL file and place it in the same directory as a legitimate Microsoft Office file. The user would then be exploited after opening the legitimate Office file.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

· Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

· Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

· Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

· Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

· Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms11-073

SecurityFocus:

http://www.securityfocus.com/bid/49513

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1980
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1982